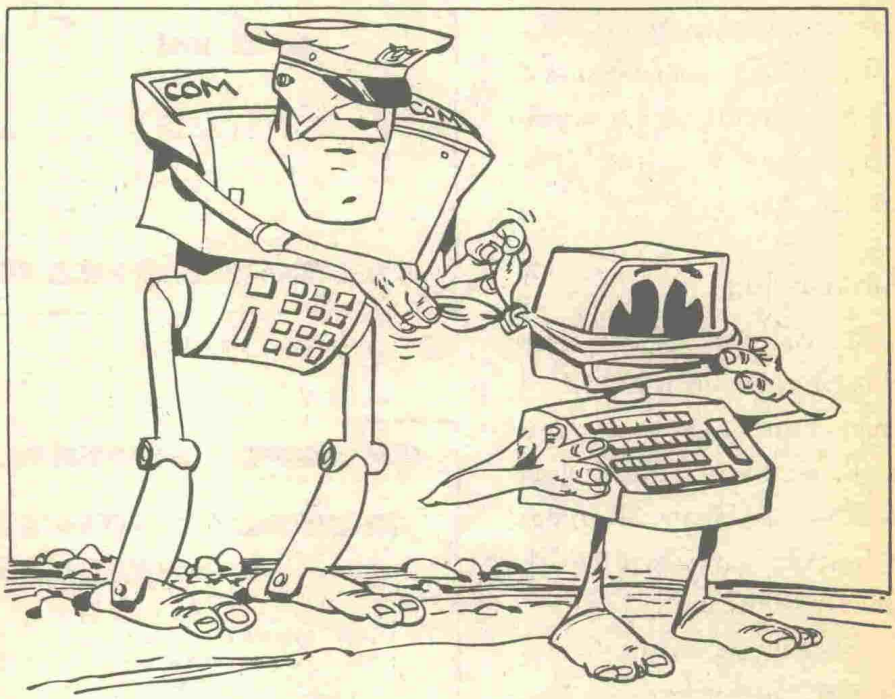
ระบบรักษาความปลอดภัย บน PC TOOLS 7.1 (2)

การใช้โปรแกรม
ที่ช่วยป้องกันไวรัส
บน Pc Tools



ตอนนี้เป็นตอนสุดท้ายของระบบรักษาความปลอดภัยบน Pc Tools 7.1 เป็นจังหวะพอดีที่ Contral Point ได้ออก Pc Tools 8.0 ให้ผู้ใช้ทั่วไปได้ใช้กัน เท่าที่ดูลักษณะการทำงานและหลักการใช้งานก็คงยังเหมือนกัน Pc Tools 7.1 อยู่ดี แต่ก็เพิ่มข้อปลีกย่อยขึ้นมาอีกนิดเดียว

Wipe

เป็นส่วนหนึ่งของ PC Tools Deluxe 7.1 ที่ใช้ทำหน้าที่ป้องกันการนำข้อมูลไปใช้ก็คือ 'Wipe' ซึ่งมันจะทำการลบข้อมูลออกจากดิสค์ให้ โดยที่การลบนี้จะเป็นการลบที่ตัวข้อมูลจริง ๆ ไม่ใช่เป็นเพียงการลบชื่อไฟล์ออกจากดิสค์ ซึ่งยังคงสามารถอ่านข้อมูลของไฟล์ที่ถูกลบแล้วนั้นได้ ถ้าพื้นที่ที่ใช้เก็บข้อมูลของไฟล์ยังไม่ได้จัดสรรไปให้ไฟล์อื่น ๆ ใช้หรือถูกเขียนทับใหม่ ฉะนั้นเมื่อเรียกใช้ Wipe แล้วก็จะทำให้ไม่สามารถอ่านข้อมูลต่าง ๆ เหล่านั้นได้อีก ซึ่งสิ่งที่จะได้รับจาก Wipe จะประกอบด้วย

– Protect Delete Files ซึ่งจะทำให้สามารถป้องกันไม่ให้มีใครสามารถเรียกดูข้อมูลที่ถูกลบทิ้งแล้วได้ ไม่ว่าจะด้วยวิธีใด

– Comply with U.S. Government Requirements เป็นขีดความสามารถของ Wipe ที่จะลบข้อมูลตามมาตรฐานของรัฐบาลสหรัฐฯได้

– Clear Unused Space เป็นการลบข้อมูลที่ถูกลบทิ้งไปแล้ว จากดิสค์ส่วนที่ไม่ใช้งานแล้วหรือจากที่ว่างระหว่างไฟล์

– Wipe Entire Directories ซึ่งสามารถจะลบไฟล์ทั้งหมดรวมทั้งไดเรคทอรีย่อย (subdirectories) ของไดเรคทอรีนั้นโดยสั่งงานเพียงครั้งเดียว

เมื่อมีการใช้คำสั่งลบไฟล์ด้วยคำสั่ง 'DEL' ของดอสระบบก็จะทำการลบชื่อไฟล์นั้นออกจากไดเรคทอรี แต่ข้อมูลของไฟล์ก็ยังคงอยู่ในดิสค์จนกว่าไฟล์อื่นจะนำเอาพื้นที่ส่วนนั้นไปใช้ซึ่ง Wipe จะลบไฟล์หรือไดเรคทอรีหรือทั้งดิสค์ โดยจะเขียนอักษรอื่น (user-definable character) ลงบนพื้นที่นั้นแทน

เมื่อจะใช้ Wipe :

ถ้าต้องการจะเรียกใช้โปรแกรม 'Wipe' ก็สามารถทำได้ด้วยการเรียกใช้จากบรรทัดรับคำสั่งของดอสโดยตรงดังนี้

```
WIPE <Enter>
```

ซึ่งก็จะปรากฏจอภาพหลักของ Wipe ให้ (ตามรูปที่ 1) และผู้ใช้สามารถที่จะเลือกรายการคำสั่งต่าง ๆ เพิ่มเติมได้อีกหลายชุดคือ File, Disk, Configure และ Exit

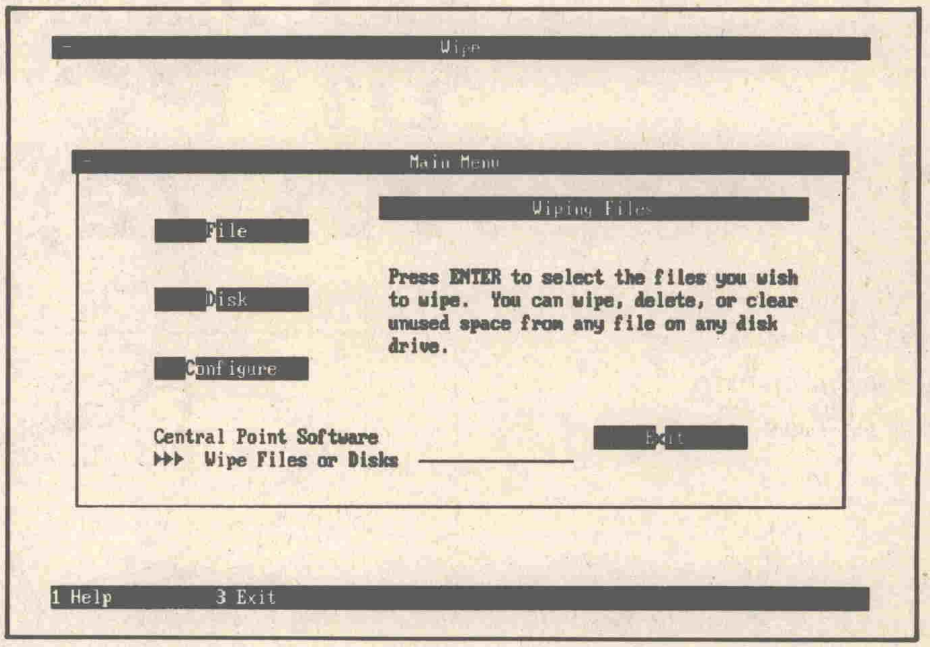
ลบไดเรคทอรี/ไฟล์ :

ในกรณีที่เป็นการติดตั้ง Wipe เป็นครั้งแรก มันจะถูกกำหนดให้ทำงาน (default) แบบ 'Fast Wipe' ซึ่งจะทำงานโดยเขียนค่า 0 (zero) กับข้อมูลที่ต้องการลบแต่ถ้าต้องการที่จะเปลี่ยนให้ใช้อักขระตัวอื่นแทน สามารถทำได้ก่อนที่จะสั่งให้ลบไฟล์

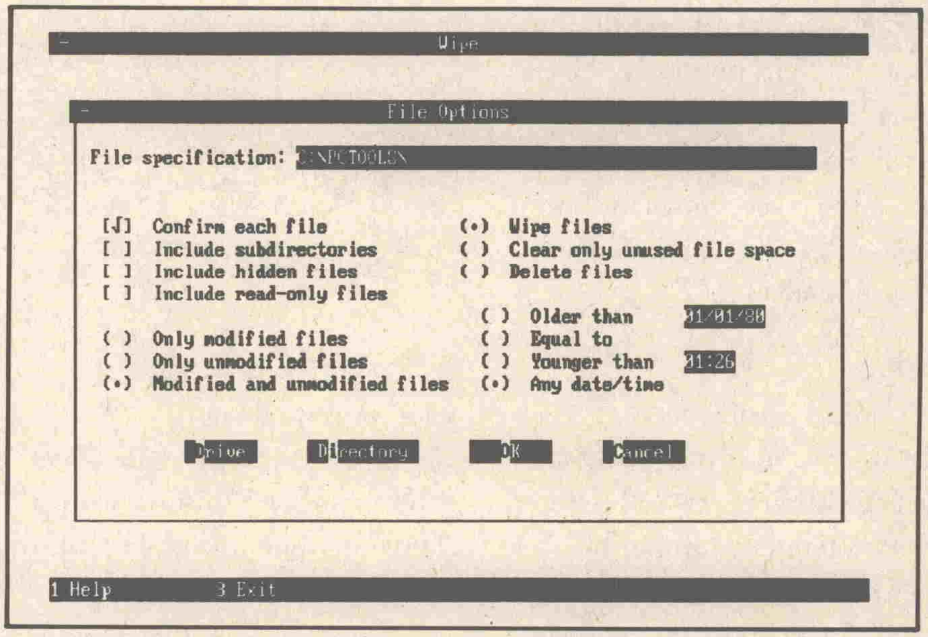
เมื่อต้องการจะลบไฟล์ ให้เลือกคำสั่ง 'File' จากจอภาพหลักของ Wipe โดยทำตามขั้นตอนต่าง ๆ ดังนี้

1. เลือกรายการ 'File' จากจอภาพหลัก ซึ่งก็จะปรากฏจอภาพของ File Options (รูปที่ 2) ให้กำหนดวิธีการต่าง ๆ ตามที่ต้องการ

2. ในส่วนของ 'File Specification' ให้พิมพ์ชื่อไฟล์ที่ต้องการลบ ซึ่งสามารถจะใช้เครื่องหมาย wildcard ของ DOS (* และ ?) ได้ถ้าต้องการลบมากกว่าหนึ่งไฟล์เช่น C:\WORD*.BAK เพื่อลบไฟล์ทั้งหมดที่มีส่วนขยายเป็น '.BAK' ที่อยู่ในไดเรคทอรี C:\WORD และถ้าไม่ได้กำหนดชื่อไดรฟ์และไดเรคทอรี Wipe ก็จะทำการลบเฉพาะไฟล์ที่อยู่ในไดรฟ์และไดเรคทอรีที่กำลังติดต่ออยู่ในขณะนั้น



รูปที่ 1 จอภาพหลักของโปรแกรม Wipe



รูปที่ 2 จอภาพของ Wipe เมื่อเรียกใช้รายการ File ในจอภาพหลัก

3. กดแป้น <Enter> เพื่อสั่งลบไฟล์ที่กำหนดไว้ ถ้าไม่ต้องการเปลี่ยนแปลงค่าอื่น ๆ ตามที่ได้แสดงให้เห็นในจอภาพ

4. ถ้าต้องการจะเปลี่ยนแปลงรายการอื่น ๆ สามารถทำได้โดยเลือกใช้รายการนั้น

– Confirm each file เป็นรายการที่จะทำหน้าที่แสดงชื่อไฟล์ที่จะทำการลบทิ้ง ซึ่งผู้ใช้สามารถที่จะสั่งให้ทำงานต่อหรือยกเลิกได้

– Include subdirectories เป็นการสั่งให้ลบไฟล์ในไดเรคทอรีย่อยของไดเรคทอรีที่ติดต่ออยู่ในขณะนั้น และมีชื่อตรงตามที่กำหนดเอาไว้

– Include hidden files จะทำหน้าที่ลบไฟล์ที่มีชื่อตามที่กำหนดไว้ ถึงแม้ว่าจะเป็นไฟล์ที่ถูกสั่งให้ซ่อนเอาไว้ (hidden file) ก็ตาม

– Include read-only files จะทำการลบไฟล์ที่ถูกกำหนดให้เป็น read-only ด้วย ถ้าชื่อไฟล์ที่กำหนดเอาไว้นั้นตรงกัน

5. เลือกชนิดของไฟล์ที่จะทำการลบได้ โดยเลือกจากรายการต่าง ๆ ดังนี้

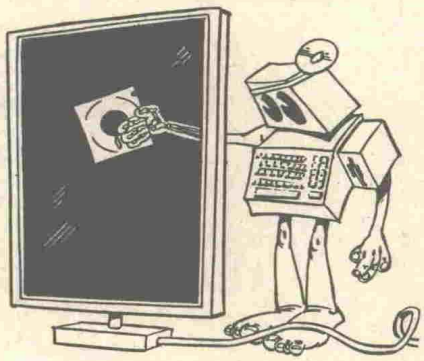
– Only modified files เป็นการสั่งให้ลบเฉพาะไฟล์ที่มีการกำหนดค่าของ archive bit ซึ่งแสดงว่าไฟล์นั้นมีการเปลี่ยนแปลงแก้ไข หลังจากที่มีการสำรอง (backup) ครั้งสุดท้ายแล้ว

– Only Unmodified files จะทำหน้าที่ลบไฟล์เฉพาะที่ไม่มีการกำหนดค่าของ archive bit ซึ่งก็คือไฟล์ที่ไม่มีการเปลี่ยนแปลงหลังจากที่ได้สำรอง (back up) ข้อมูลเอาไว้ในครั้งสุดท้าย

– Modified and unmodified files เป็นรายการที่จะทำหน้าที่ลบไฟล์ไม่ว่าไฟล์นั้นจะมีการกำหนดค่าของ archive bit หรือไม่ก็ตาม

6. เลือกรูปแบบการลบที่ต้องการได้จากรายการต่อไปนี้

– Wipe files จะเป็นการสั่งให้ลบไฟล์จากดิสก์ แล้วเขียนทับพื้นที่นั้นด้วยอักขระตามที่เลือกเอาไว้



– Clear only unused file space จะทำการลบเฉพาะส่วนของดิสก์ที่ไม่ได้ใช้งาน โดยจะไม่ลบไฟล์ที่ได้กำหนดชื่อเอาไว้ ในการทำงานของดอสนั้น จะทำการจัดสรรเนื้อที่ดิสก์ให้กับไฟล์ต่าง ๆ เป็นจำนวนคลัสเตอร์ (ซึ่งขนาดของคลัสเตอร์จะขึ้นอยู่กับดิสก์แต่ละชนิด) ซึ่งทำให้มีเนื้อที่ว่างบางส่วนเหลืออยู่ (ไม่ได้ทำไปใช้งานจริง) ตัวอย่างเช่นถ้าไฟล์มีขนาด 1,000 ไบต์ และจะนำไปเก็บในดิสก์ที่มีการแบ่งเซกเตอร์ขนาด 512 ไบต์ต่อเซกเตอร์ ดอสจะจัดสรรเนื้อที่ให้ไฟล์นี้เป็นจำนวน 2 คลัสเตอร์ (1,024 ไบต์) ซึ่งจะทำให้มีเนื้อที่ว่างที่ไม่ได้นำไปใช้งานจริง เป็นจำนวน 24 ไบต์และพื้นที่ในส่วนนี้ก็อาจจะมีข้อมูลของไฟล์ที่ถูกลบทิ้งไปแล้วอยู่ก็ได้ ฉะนั้นเมื่อที่จะลบข้อมูลในส่วนนี้ออกไปจากดิสก์ จะต้องใช้วิธีกำหนดชื่อไฟล์เป็น '*.*' โดยจะต้องเลือกใช้รายการ 'Include subdirectories' เอาไว้ด้วย

– Delete files เป็นการสั่งให้ลบไฟล์ในลักษณะการทำงานแบบเดียวกับคำสั่ง 'DEL' ของ DOS

7. เลือกไฟล์ที่ต้องการจะลบออกโดยใช้วันเวลาที่สร้างไฟล์ซึ่งก็จะมีรายการให้เลือกดังนี้

– Older than เป็นการเลือกไฟล์ที่มีวัน/เวลาเดียวกันหรือก่อนวัน/เวลาที่กำหนด

– Equal to เป็นการกำหนดไฟล์ที่มีวัน/เวลา เดียวกันกับที่กำหนดเอาไว้

– Younger then เป็นการสั่งให้ลบเฉพาะไฟล์ที่มีวันที่/เวลาหลังจากที่กำหนดเอาไว้

– Any date/time เป็นทางเลือกให้ลบไฟล์โดยไม่ต้องสนใจกับวันที่/เวลาที่สร้างไฟล์นั้น

8. เลือกคำสั่ง 'OK' เพื่อให้โปรแกรมทำงานต่อไป ซึ่งก็จะปรากฏจอภาพเตือนให้รู้ก่อนที่จะเริ่มทำงานจริง (ตามรูปที่ 3)

9. ถ้าได้มีการเลือกรายการ 'Confirm each file' เอาไว้ในขั้นตอนที่ 4 ก็สามารถที่จะเลือกไฟล์ที่ต้องการลบได้

– Skip เป็นทางเลือกที่จะให้ยกเลิกการลบไฟล์ที่ติดต่ออยู่ในขณะนั้น โดยข้ามไปที่ไฟล์ลำดับถัดไป

– Wipe เป็นการสั่งให้ลบไฟล์ที่กำลังติดต่ออยู่ขณะนั้น แล้วจึงเลื่อนต่อไปที่ไฟล์ในลำดับถัดไป

ซึ่งก็จะปรากฏจอภาพ (dialog box) แสดงให้เห็นชื่อไฟล์ที่ถูกลบออกไปจริง ๆ หรือลบออกแบบปกติ หรือข้ามไปโดยไม่ลบ

วิธีเปลี่ยนไดรฟ์ :

ในกรณีที่ต้องการจะเปลี่ยนไดรฟ์ใช้งานก็จะสามารถทำได้ตามขั้นตอนดังนี้

1. เลือกรายการ 'Drive' จาก File Option dialog box

2. เลือกไดรฟ์ที่มีไฟล์ที่ต้องการลบ แล้วเลือกคำสั่ง 'OK' ซึ่งก็จะมีการแสดง File Specification text box ให้เห็นรายการที่ได้เลือกเอาไว้

เปลี่ยนไดเรคทอรี :

การเปลี่ยนไดเรคทอรีที่ต้องการจะใช้ทำงาน สามารถทำได้ด้วยขั้นตอนต่อไปนี้

1. เลือกรายการ 'Directory' จาก File Option

– ถ้าต้องการเลือกไดเรคทอรีในระดับที่สูงกว่า ให้เลือกบรรทัดที่มีเครื่องหมาย ' . ' (period) 2 ตัว

– ถ้าจะเปลี่ยนให้เป็นไดเรคทอรีย่อยในระดับต่ำกว่า ให้เลือกชื่อไดเรคทอรี ซึ่งชื่อของไดเรคทอรีในระดับต่ำกว่าจะมีคำว่า <DIR> ต่อท้ายชื่อ

2. เลือกคำสั่ง 'OK' เมื่ออยู่ในไดเรคทอรีที่ต้องการแล้ว หลังจากเสร็จขั้นตอนนี้ จะปรากฏ File Specification text box แสดงทางเลือกที่ได้ทำไว้

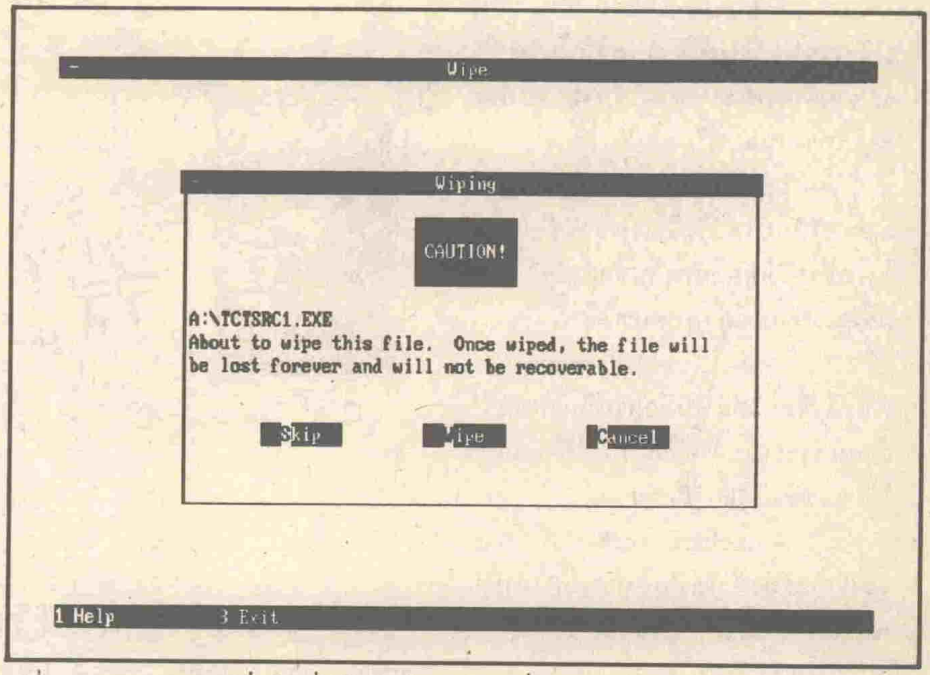
เมื่อจะลบดิสค์ :

ในการเรียกใช้โปรแกรม Wipe นั้น ถ้าเป็นการติดตั้งครั้งแรกก็จะถูกกำหนดให้ทำงานในแบบ 'Fast Wipe' โดยใช้ค่า 0 (zero) แทนข้อมูลที่ถูกลบ และจะมีขั้นตอนการทำงานดังนี้

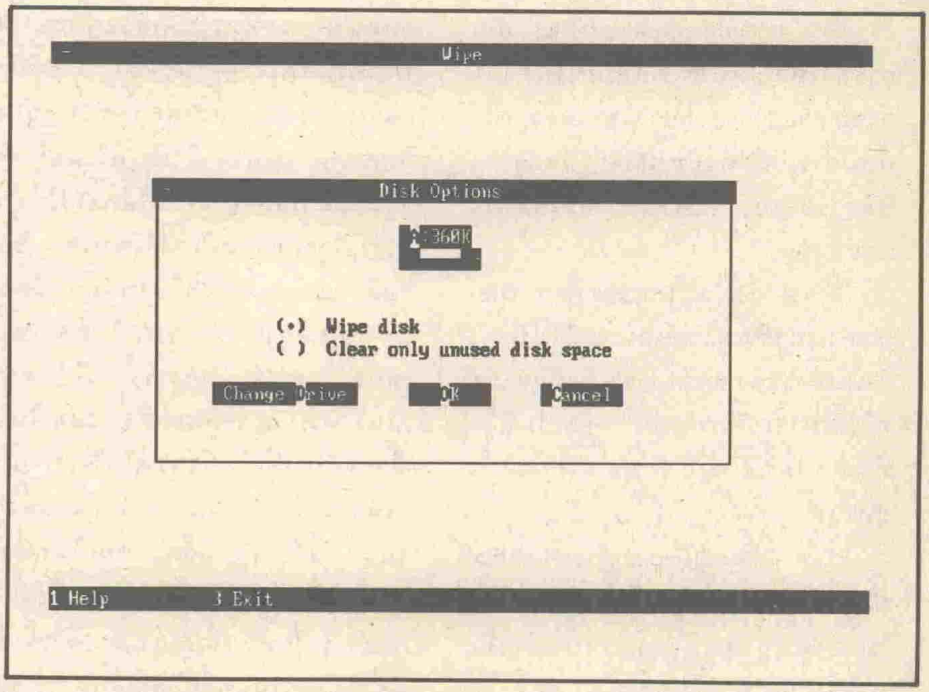
1. เลือกใช้รายการ 'Disk' จากจอภาพหลักของ Wipe ซึ่งก็จะปรากฏจอภาพของ Disk Option ให้ ตามรูปที่ 4

2. ถ้าต้องการเปลี่ยนไดรฟ์ ก็ให้เลือกรายการ 'Change Drive' และเลือกไดรฟ์ที่ต้องการแล้วจึงใช้คำสั่ง 'OK'

3. เลือกส่วนของดิสค์ที่ต้องการลบ จากรายการต่าง ๆ ดังนี้



รูปที่ 3 จอภาพของ Wipe เมื่อมีการสั่งให้ลบไฟล์จากรายการคำสั่งของ File Option



รูปที่ 4 จอภาพของ Wipe เมื่อเรียกใช้รายการ Disk จากจอภาพหลัก

– Wipe disk จะเป็นการสั่งให้ลบหมดทั้งดิสค์

– Clear only unused space เป็นทางเลือกที่จะลบเฉพาะส่วนของข้อมูลที่ถูกลบทิ้ง ซึ่งจะไม่มีผลต่อไฟล์ที่เหลืออยู่

4. เลือกคำสั่ง 'OK' ซึ่งหลังจากการยืนยันความต้องการให้ 'Wipe' ทำงานต่อจะมีการแสดงความก้าวหน้าในระหว่างการทำงานให้เห็นบนจอภาพด้วย

5. การยกเลิกคำสั่งให้ลบดิสค์ ก็ทำได้ด้วยการเลือกคำสั่ง 'Stop' แล้วจึงเลือกคำสั่ง 'Cancel' ต่อไป

ทางเลือกของ Wipe :

การใช้งานโปรแกรม 'Wipe' นี้ ผู้ใช้สามารถที่จะกำหนดหรือควบคุมการทำงานได้ด้วย ซึ่งถ้าต้องการที่จะเปลี่ยนแปลงวิธีการทำงานให้แตกต่างไปจากที่ได้กำหนดเอาไว้ให้ก่อนแล้ว (default) สามารถทำได้ตามขั้นตอนต่อไปนี้

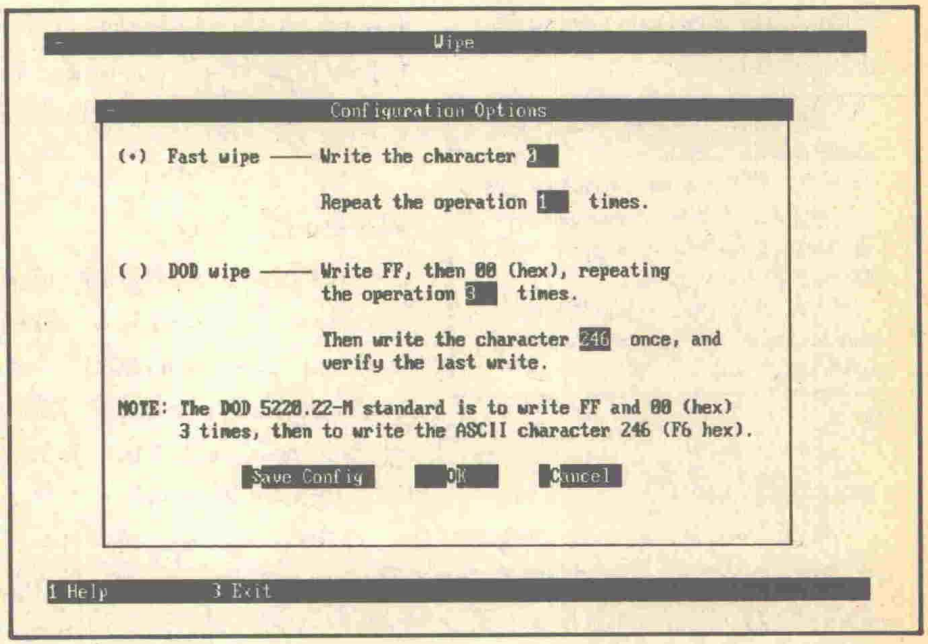
1. เลือกใช้รายการ 'Configure' จากจอภาพหลักของ Wipe ซึ่งก็จะปรากฏจอภาพของ 'Configuration Options' ให้ตามรูปที่ 5

2. เลือกวิธีการทำงานของ 'Wipe' ตามระดับความปลอดภัยที่ต้องการ

– FastWipe เป็นทางเลือกที่จะให้เขียนทับพื้นที่ที่ต้องการลบ ด้วยอักขระ (charactor) ที่กำหนดเอาไว้

– DOD Wipe เป็นการกำหนดให้ใช้วิธีการลบตามมาตรฐานของ U.S. Department of Defense ซึ่งผู้ใช้สามารถกำหนดจำนวนครั้งที่ต้องการให้เขียนทับพื้นที่ที่ต้องการลบด้วยค่า 1 และ 0 (จำนวนครั้งขั้นต่ำสุดคือ 3) นอกจากนี้ยังสามารถใช้ค่า (ASCII number) ของตัวอักขระที่ต้องการใช้ได้ด้วย

3. ถ้าเลือกใช้วิธีการแบบ 'Fast Wipe' และต้องการให้ทำงานมากกว่าหนึ่งครั้งเพื่อให้มีความปลอดภัยมากขึ้น ก็สามารถใส่จำนวนครั้งที่ต้องการได้ระหว่าง 1-999 เอาไว้ในรายการ 'Repeat the operation'



รูปที่ 5 จอภาพของ Wipe เมื่อเรียกใช้รายการ Configure จากจอภาพหลัก

4. ในกรณีที่ต้องการใช้ค่าที่ตั้งเอาไว้นี้ในโอกาสต่อไป ก็ให้เลือกใช้รายการ 'Save Config' แต่ถ้าไม่ต้องการก็ให้เลือกคำสั่ง 'OK' เพื่อทำงานต่อไป

สั่งงานจาก Command-line :

การใช้งาน 'Wipe' นั้นสามารถที่จะทำจากบรรทัดรับคำสั่งดอสได้โดยตรง (ไม่ต้องทำผ่านจอภาพหลักของ Wipe) ซึ่งการสั่งงานด้วยวิธีนี้จะมีรูปแบบ (syntax) ดังนี้

```
WIPE d: [/DISK][/UNUSED][/GOVT] [/REP:n][/VALUE:n]
หรือ
WIPE [d:] filespec [/DELETE][/SUB] [/HIDDEN]
[/READONLY][/MODIFIED or/UNMODIFIED]
[/NOCONFIRM][/UNUSED][/GOVT] [/REP:n]
[/VALUE:n]
```

ซึ่งถ้าเป็นการใช้คำสั่งเพื่อลบดิสค์ก็จะมีทางเลือกให้ 2 ทางคือ

d: เพื่อใช้กำหนดไดรฟ์ที่ต้องการลบ

/DISK เป็นการสั่งให้ลบทั้งดิสค์ (เป็นค่า default ด้วย)

แต่ถ้าต้องการใช้งานกับไฟล์ก็จะมีทางเลือกให้หลายทางดังรูปที่ 6

d: เป็นไดรฟ์ที่เก็บไฟล์ที่ต้องการลบออก

filespec เป็นชื่อไฟล์ที่ต้องการลบ ซึ่งสามารถจะใช้เครื่องหมาย wildcard (* และ ?) ของ DOS เพื่อกำหนดกลุ่มของไฟล์ที่ต้องการได้

/DELETE เป็นการสั่งให้ลบไฟล์โดยไม่ต้องลบข้อมูลของไฟล์ออกด้วย

/SUB ให้ลบไฟล์ที่อยู่ในไดเรคทอรีย่อยด้วย

/HIDDEN ลบ hidden file ที่มีชื่อตรงกันด้วย

/READONLY ลบไฟล์ที่กำหนดชื่อไว้รวมทั้งไฟล์ที่กำหนดให้เป็น read-only ด้วย

/MODIFIED ให้ลบเฉพาะไฟล์ที่ถูกแก้ไขหลังจากการสำรอง (backup) ครั้งสุดท้ายแล้ว

/UNMODIFIED ลบเฉพาะไฟล์ที่ไม่ถูกแก้ไขหลังจากที่ได้สำรองเอาไว้ครั้งสุดท้าย

/NOCONFIRM เป็นคำสั่งให้ลบไฟล์โดยไม่ต้องรอคำยืนยันให้ลบแต่ละไฟล์

รูปที่ 6

ส่วนทางเลือกสำหรับการใช้งานทั่ว ๆ ไปนั้นก็จะมีดังรูปที่ 7

/UNUSED เป็นคำสั่งให้ลบเฉพาะช่องว่างของไฟล์หรือดิสค์ที่ไม่ได้ใช้งาน

/GOVT ให้ทำงานตามกฎเกณฑ์ของ DoD

/REP:n ใช้กำหนดจำนวนครั้งที่ต้องการให้ทำซ้ำ โดยใส่จำนวนครั้งที่ต้องการแทนอักษร 'n' ซึ่งค่าที่กำหนดไว้ให้ (default) คือ 1

/VALUE:n ทำหน้าที่กำหนดอักขระที่ต้องการให้เขียนแทนข้อมูลที่ถูกลบ โดยใส่ไว้แทนอักษร 'n' ส่วนค่าที่กำหนดไว้ให้คือ 0

รูปที่ 7

ทางเลือกที่ใช้ร่วมกันได้ :

ทางเลือกการทำงานของ 'Wipe' ที่มีอยู่เป็นจำนวนมากนั้นมีบางตัวที่สามารถที่ใช้งานร่วมกันได้ ในขณะที่บางตัวก็ไม่สามารถกำหนดให้ทำงานพร้อมกันได้ ฉะนั้นถ้าต้องการที่จะใช้งานพารามิเตอร์หลาย ๆ ตัวด้วยกัน ก็จะต้องพิจารณาดูว่าพารามิเตอร์เหล่านั้นสามารถทำงานร่วมกันได้หรือไม่ ซึ่งกลุ่มของพารามิเตอร์ที่ใช้งานด้วยกันได้นั้น ได้แสดงเอาไว้ในรูปที่ 8 โดยเครื่องหมาย '*' จะแสดงถึงการใช้งานร่วมกันได้ระหว่างตัวพารามิเตอร์ที่อยู่ในแถว (row) และคอลัมน์ (column) นั้น

VDefend

เป็นโปรแกรมที่ทำงานแบบฝังตัวในหน่วยความจำ (memory-resident program) เพื่อคอยทำหน้าที่ป้องกันไม่ให้ระบบคอมพิวเตอร์ติดไวรัสได้มากกว่า 400 ชนิด ส่วนวิธีการป้องกันก็จะมีรูปแบบอยู่ 2 อย่างคือ

- Checks Executable Files For Infection ซึ่งจะทำหน้าที่ตรวจสอบไวรัสที่มันรู้จัก เมื่อมีการประมวลผลหรือสำเนา (copy) ไฟล์ที่สามารถประมวลผลได้ (executable files) ซึ่งถ้าพบว่ามีไวรัสก็จะแสดงข่าวสารให้รู้ ส่วนการกำจัดนั้นอาจใช้โปรแกรม Anti-Virus ของ Central Point Software ซึ่งเป็นอีกโปรแกรมหนึ่งแยกต่างหาก

- Prevents Unauthorized Formatting คือการทำหน้าที่ป้องกันการฟอร์แมตดิสค์ โดยจะเตือนให้รู้เมื่อมีการพยายามที่จะฟอร์แมตดิสค์ในแบบ Low-level format ซึ่งมีไวรัสหลาย ๆ ชุดที่มักจะทำลายข้อมูลในดิสค์ด้วยวิธีนี้ และผู้ใช้สามารถที่จะตัดสินใจให้ทำงานต่อไปหรือหยุดการทำงานนั้นได้

Option Combinations

	DISK	UNUSED	SUB	GOVT	REP	VALUE	HIDDEN	MODIFIED	UNMODIFIED	DELETE	NOCONFIRM	READONLY
DISK		*		*	*	*						
UNUSED	*		*	*	*	*	*	*	*		*	*
SUB		*		*	*	*	*	*	*	*	*	*
GOVT	*	*	*		*	*	*	*	*		*	*
REP	*	*	*	*		*	*	*	*		*	*
VALUE	*	*	*	*	*		*	*	*		*	*
HIDDEN		*	*	*	*	*		*	*	*	*	*
MODIFIED		*	*	*	*	*	*			*	*	*
UNMODIFIED		*	*	*	*	*	*			*	*	*
DELETE			*				*	*	*		*	*
NOCONFIRM		*	*	*	*	*	*	*	*	*		*
READONLY		*	*	*	*	*	*	*	*	*	*	

รูปที่ 8 รายการพารามิเตอร์ของคำสั่ง Wipe ที่ใช้ร่วมกันได้

โปรแกรม 'VDefend' เป็นเครื่องมือที่จะช่วยให้ผู้ใช้รู้ว่ามีการทำงานของไวรัสที่รู้จักเท่านั้น โดยจะไม่ทำการกำจัดให้ ถ้าต้องการที่จะทำการค้นหาและกำจัดไวรัสก็จะต้องใช้โปรแกรมชุดอื่นที่สามารถทำงานในลักษณะนี้ได้ ซึ่งก็รวมทั้ง Central Point Anti-Virus ที่เป็นผลงานของผู้ผลิตรายเดียวกันนี้ด้วย โดยมันจะมีขีดความสามารถในการจัดการกับไวรัสได้อย่างดี (เป็นผลิตภัณฑ์ที่ได้รับเลือกให้เป็น "Editor's Choice" ของ PC Labs ประจำเดือนตุลาคม 1991 ซึ่งรวมถึงความสามารถในการกำจัดไวรัสและซ่อมไฟล์ที่ติดไวรัสด้วย

นอกจากนี้ผู้ใช้ยังสามารถเปลี่ยนชุด (up date) ของ 'VDefend' ได้ด้วยการสำเนา (download) ไฟล์ (virus signature file) ชื่อ 'SIGNATUR.CPS' จาก BBS ของ Central Point ได้ หรืออาจใช้บริการจาก CompuServe ในส่วนของ Central Point Forum ก็ได้ ซึ่งวิธีการก็เพียงแต่สำเนาไฟล์เข้าไปเก็บไว้ในไดเรคทอรีที่ติดตั้ง 'VDefend' เอาไว้เท่านั้น

เรียกใช้ VDefend :

ผู้ใช้สามารถที่จะเรียกใช้ 'VDefend' ให้ทำงานได้ทันทีเมื่อเปิดเครื่องคอมพิวเตอร์ โดยใส่คำสั่งเพื่อเรียกใช้โปรแกรมนี้เอาไว้ในไฟล์ 'AUTOEXEC.BAT' ซึ่งวิธีการใส่ชุดคำสั่งนี้ก็จะมีดังต่อไปนี้

1. ใช้โปรแกรม 'Install' ของ Central Point เพื่อให้สามารถเรียกใช้ 'VDefend' ได้จากไฟล์ 'AUTOEXEC.BAT'

2. เรียกใช้ระบบ (boot) ใหม่ โดยกดแป้น <Ctrl><Alt><Del> ซึ่งจะทำให้มีการเรียกใช้ (load) 'VDefend' โดยอัตโนมัติ

เมื่อพบไวรัส :

วิธีการที่ VDefend จะใช้เมื่อพบว่ามีไวรัส เข้ามาในระบบคอมพิวเตอร์นั้นจะมีอยู่ 2 อย่าง ซึ่งแต่ละวิธีก็จะมีขั้นตอนการทำงานดังนี้

* ในกรณีที่พบว่ามีไวรัสแพร่เข้าสู่ระบบคอมพิวเตอร์ขณะที่กำลังประมวลผลโปรแกรมใดอยู่ก็จะแสดงข้อความให้เห็นบนจอภาพ เพราะทุก ๆ ครั้งที่มีการเรียกใช้ไฟล์ที่สามารถประมวลผลได้ (เช่น .EXE หรือ .COM) VDefend ก็จะทำการตรวจสอบว่ามีไวรัสที่รู้จักหรือไม่ ส่วนวิธีการจัดการกับไฟล์ที่ติดไวรัสคือ ควรจะลบทิ้งไปแล้วติดตั้งใหม่จากแผ่นต้นฉบับ และถ้าเป็นไปได้ก็ควรจะใช้โปรแกรม antivirus (ชุดไหนก็ได้ที่คุณมี แต่ควรจะเป็นโปรแกรมที่มีขีดความสามารถสูงหน่อยเพื่อความปลอดภัยของระบบ) ตรวจสอบไวรัสในระบบอีกครั้ง

* การค้นพบไวรัสอีกวิธีหนึ่ง ซึ่งอาจจะเจอเมื่อพบว่ามีความพยายามที่จะฟอร์แมตดิสก์ (low-level formatting) เพราะมีไวรัสบางชุดที่จะสร้างความเสียหายให้กับระบบคอมพิวเตอร์ด้วยการฟอร์แมตฮาร์ดดิสก์ และในกรณีนี้ VDefend ก็จะเตือนให้รู้ว่ามีความพยายามจะฟอร์แมตดิสก์ ซึ่งจะทำให้ข้อมูลในดิสก์สูญหายหมดและไม่สามารถจะกู้คืนได้ถึงแม้ว่าจะใช้โปรแกรมที่มีความสามารถสูงก็ตาม แต่เหตุการณ์ในลักษณะนี้ก็มีข้อยกเว้นเช่นกัน คือ ถ้าเป็นการสั่งฟอร์แมต (low-level format) จากโปรแกรม Diskfix ของ PC Tools เอง ก็สามารถสั่งให้ทำงานต่อได้ เพราะโปรแกรมนี้จะไม่ทำลายข้อมูลที่มีอยู่เดิมในระหว่างการทำงาน ซึ่งขั้นตอนการสั่งงานจะเป็นดังนี้

- ถ้าต้องการให้ทำงานต่อก็เลือกคำสั่ง Continue ซึ่งก็จะมีผลให้มีการฟอร์แมตดิสก์ต่อไป
- เมื่อไม่ต้องการให้มีการฟอร์แมตดิสก์ ก็ให้เลือกคำสั่ง Stop ซึ่งจะทำให้ VDefend ส่งข่าวสารความผิดพลาด (error message) ไปให้โปรแกรมที่สั่งฟอร์แมต เพื่อบอกให้รู้ว่าไม่สามารถทำการฟอร์แมตได้
- ถ้าการสั่งด้วย Stop ไม่สามารถหยุดการทำงานได้ ก็ให้เลือกคำสั่ง Boot เพื่อให้ VDefend เรียกใช้ระบบใหม่ (reboot)

สิ่งสุดท้ายที่ควรทำเมื่อพบว่ามีความพยายามจะฟอร์แมตฮาร์ดดิสก์อย่างไม่ถูกต้อง (แสดงว่าเจอไวรัสแล้ว) คือ หาโปรแกรม antivirus มาตรวจสอบระบบอีกครั้งเพื่อความแน่ใจ

ยกเลิกการใช้ VDefend:

ในบางกรณีผู้ใช้อาจต้องการใช้พื้นที่ในหน่วยความจำมากขึ้น ซึ่งอาจจำเป็นจะต้องเรียกหน่วยความจำบางส่วนคืนจากโปรแกรม TSR (Terminate-and-stay-resident program ทั้งหลายที่จับจองพื้นที่บนส่วนเอาไว้ และ VDefend ก็อาจเป็นหนึ่งในจำนวนนั้นด้วย ฉะนั้นถ้าต้องการจะเอา VDefend ออกจากหน่วยความจำก็สามารถทำได้ตามขั้นตอนต่อไปนี้

1. จะต้องจัดการยกเลิกการใช้งาน TSR ทั้งหมดที่เรียกใช้ (load) หลังจากเรียกใช้ VDefend ก่อน

2. สั่งยกเลิกการใช้งาน VDefend จากบรรทัดรับคำสั่งของดอส

```
VDEFEND /U <Enter>
```

หรือถ้าต้องการยกเลิกโปรแกรม TRS ทั้งหมดของ PC Tools ก็สามารถจะทำได้ตามวิธีการดังนี้

1. จะต้องยกเลิกการใช้งานโปรแกรมทั้งหมดของ PC Tools ที่ไม่ใช่โปรแกรมประเภท TSR ที่เรียกใช้ต่อจาก PC Tools

2. ใช้ยกคำสั่งยกเลิก TSR ทั้งหมดจากดอส

```
KILL <Enter>
```

ก่อนจาก

เรื่องราวของระบบการรักษาความปลอดภัยในการใช้เครื่องคอมพิวเตอร์ PC Tools Deluxe 7.1 ที่นำมาพูดคุยกัน ต้องจบลงด้วยประการฉะนี้ แต่เรื่องราวของ PC Tools ยังไม่ได้จบตามลงไปด้วย เพราะยังมีเรื่องที่น่าสนใจอีกหลายเรื่องและสิ่งที่จะนำมาเล่าให้ฟังในคราวต่อไป จะเกี่ยวกับงานของ PC Tools ในส่วนของการจัดการบางอย่างกับระบบคอมพิวเตอร์ ก็คือ การตรวจสอบระบบ (System Information) การดูแลและจัดการกับไดเรคทอรี (Directory Maintenance), ระบบการค้นหาไฟล์ และการเข้าไปดูข้อมูล (contents) ที่อยู่ในไฟล์ที่มีการจัดเก็บข้อมูลในแบบต่าง ๆ โดยที่ทั้งหมดนี้เป็นบางส่วนที่เป็นคุณสมบัติของ PC Tools ในเรื่องของการจัดการระบบ แต่ก็เป็นส่วนที่เพิ่มเข้ามาใหม่ในเวอร์ชันนี้ คุณเป็นคนหนึ่งที่สนใจโปรแกรม PC Tools Deluxe ก็ขอให้คอยติดตามกันต่อไป ซึ่งก็คงจะไม่นานเกินรอหรอกครับ